

MENU

Mobile Security

Data Protection

Identity & Access

CSOM

New cryptocurrencies offer better anonymity, new security challenges

Anonymous cryptocurrencies like Monero and Zcash help cybercriminals evade detection and make cryptojacking more profitable.

Maria Korolov (CSO (US)) on 01 February, 2018 22:00

0 Comments

0



A new crop of anonymous cryptocurrencies, which are less traceable and offer greater privacy than Bitcoin, are gaining ground with cybercriminals. Despite the lower risk of being caught that cryptocurrencies like Monero and Zcash offer, Bitcoin remains the currency of choice for [ransomware](#) payments because it's easier for the public to acquire.

The biggest impact that anonymous cryptocurrencies have on enterprises, at least in the short term, is that criminals are hijacking their computers to mine the currency. "If you're doing something illegal like cryptojacking to make a profit, the money will only be good to you if you can stay out of jail," says Bryan York, director of services at CrowdStrike, Inc.

Plus, Monero cryptojacking is easier to carry out than Bitcoin mining. Bitcoin is a mature and crowded ecosystem, and miners typically need specialized computing equipment to make any money. Monero is intended to be mined by regular computers, says Mike Price, CTO at cybersecurity vendor ZeroFox. That means the mining isn't concentrated in a few big mining operations, but distributed more widely across people's personal computers.

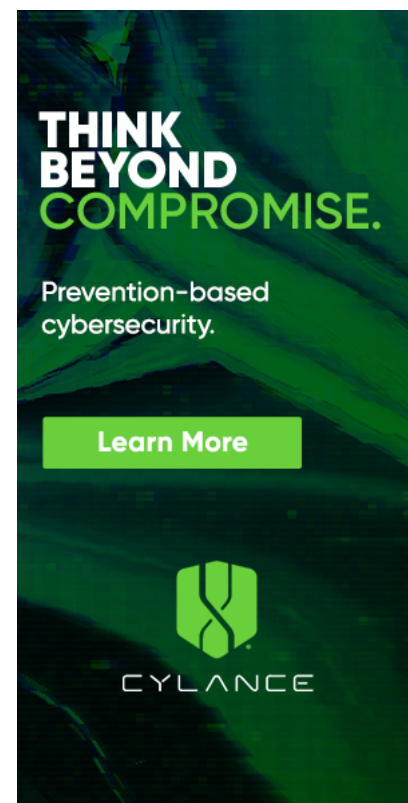
There's a downside, he says. "It incentivizes attempts to mine on personal computing devices without the direct consent of the device owner." In other words, cryptojacking.

Cryptojacking turns devices into cryptocurrency-mining botnets

Monero, for example, can run in JavaScript on a user's computer. "It makes infecting devices and creating a [botnet](#) or exploiting browsers for mining very attractive," says Andy Norton, director of threat intelligence at Lastline, Inc., a malware protection vendor.

In fact, according to Norton, there's been a big rise in Monero mining pools lately. [Lastline tracked](#) which domains are requested by cryptojacking malware, and seven of the top eight are for Monero, while only one is for Bitcoin.

The [price of Monero](#) has been rising at a corresponding rate, says Norton. Monero was just \$12 a year ago, and recently hit a high of \$466, although it has fallen to \$271 at this writing. Monero has a market capitalization of more than \$7 billion, up from \$163 million a year ago.



Featured Whitepapers



How to Enhance Your Security Team



CSO Security Buyers Guide 2016



CSO Security Buyers Guide 2015



How to stay protected against ransomware

Monero is the only anonymous currency to crack the list of top twenty cryptocurrencies. As of this writing, it is the thirteenth largest. Zcash is number 26.

Servers, desktops, even browsers vulnerable to cryptojacking

Enterprises should watch out for cryptomining payloads on end user devices, on servers, and in browsers. "There are some very simple behavioral patterns that these types of malware display," says Norton. "Those organizations that have a layered malware analysis platform will be able to intercept when they encounter them."

Anonymous cryptocurrency malware also uses evasion technologies such as TOR or peer-to-peer file sharing to hide their communications. "Enterprises must understand that when they allow these types of technologies into the organization, they are bringing additional signals and risks that need to be monitored," says Rod Soto, director of security research at Jask, a San Francisco-based cybersecurity vendor.

Jonathan Tomek, senior director of threat research at LookingGlass Cyber Solutions, Inc., suggests that companies keep an eye out for sudden spikes in CPU usage or traffic to known cryptojacking domains.

It's not as easy to infect a server with cryptojacking malware as it is to hijack a browser, Tomek says. If it happens, it's probably the least of a company's problems. "But it's probably a very good early warning indication," he says.

For browser-based cryptojacking attacks, one approach is to turn off JavaScript, Tomek says. "But that's not always an option in many places because it's a backbone for so many web pages or internal applications," he says.

Making cryptocurrencies harder to track



When it comes to security analytics, too much data still isn't enough

[More from LogRhythm »](#)

Bitcoin is based on a public ledger with every single transaction out there for everyone to see. It still takes a bit of shoe leather to identify the owner of any particular Bitcoin wallet, and criminals have other tools to hide their identities as well.

For example, ransomware authors can create a separate wallet for each victim to make life more difficult for security researchers, or use "mixer" services to disguise the movement of funds. However, the Bitcoin ecosystem is coming under increased scrutiny of regulators, and it's getting harder and harder for the bad guys to cash out their ill-gotten gains, experts say.

"The authorities can follow the trail of Bitcoins though the blockchain until they are exchanged for another 'real world' currency and then force the exchanges to reveal the identity of the customer," says Chris Camejo, director of product management for threat intelligence at NTT Security.

In addition, Bitcoins can also be traced back to their origins or to a particular public cybercrime. "Any bitcoins used in a criminal transaction could be tainted and addresses can be blacklisted," says Nick Bilogorskiy, cybersecurity strategist at Juniper Networks, Inc.

Just last week, [Europol held a workshop](#) in which investigators from 32 different countries got together and agreed to take action against digital currency mixers and to regulate exchanges and wallet providers under anti-money laundering and counter-terrorism laws. "The ransomware authors are catching on that people are watching the Bitcoin wallets," says Andrew Howard, CTO at Kudelski Security.

Editor's Recommendations



Collaboration is key to getting cyber insurance right



New year provides enterprises prime opportunity to recalibrate security posture

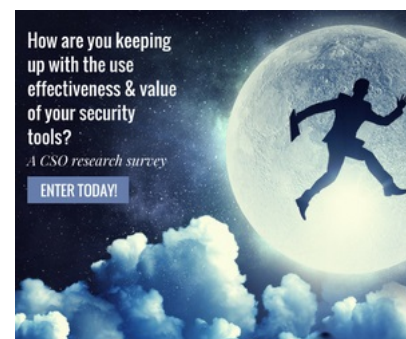


Online analytics firms leak user passwords from sites

Solution Centres



The Australian Mandatory Data Breach Notification Resource Centre



Stories by Maria Korolov

The global cyber war is heating up: Why businesses should be worried

New cryptocurrencies offer better anonymity, new security challenges

Password managers grow up, target business users

What is a botnet? And why they aren't going away anytime soon

Latest Videos



Monero disguises the origin, destination and amount of each transaction. Zcash does something similar, but uses the zero-knowledge algorithm instead of Monero's proof-of-work algorithm, and is believed to offer more privacy as a result.

Because of the added complexity, the transactions take longer. Very large transactions still make a splash, so criminals would need to break them up into smaller ones that are harder to track. As a result, cryptocurrency transactions take longer to execute and require more processing, so they're not likely to become the go-to online payment method.

They are gaining ground for criminal-to-criminal commerce, and to launder money collected via Bitcoin or other methods. For example, the criminals behind the [WannaCry](#) ransomware attack collected their Bitcoin from their victims, then converted them to Monero to hide their tracks, says David Shear, analyst at cybersecurity vendor Flashpoint. "With one hop, and now you can't track it," he says. "Now you'll see criminals launder everything through anonymous cryptocurrency."

It's also showing up on the [dark web](#), experts say. "Monero is already being integrated into multiple darknet markets, has been used in cybercrime campaigns, and is the preferred currency of the Shadow Brokers," says Benjamin Brown, engineer on the security intelligence and response team at Akamai Technologies, Inc. "I expect to see wider underground adoption going forward, especially among new darknet markets."

Monero got a big publicity boost last summer when authorities shut down the AlphaBay dark web marketplace, which was ten times larger than Silk Road. AlphaBay also accepted Bitcoin, Ethereum, and Zcash for its transactions. [Prosecutors reported](#) that they were able to seize about \$8.8 million worth of Bitcoin, Ethereum, and Zcash, and "an unknown amount of Monero."

"Authorities could not find out anything about the Monero transactions, so it gave Monero a big boost," says Mike Stute, chief scientist at Masergy Communications, Inc. "It was Monero's proof that it works."

The anonymity is a double-edged sword, however, since the virtual currency infrastructure itself also becomes more vulnerable. "If cryptocurrency exchanges start dealing these anonymous cryptocurrencies, then they can become a target for hackers," says Stephen Giguere, security strategist at Synopsys, Inc. "The hackers know that stealing this currency will keep them anonymous."

Plus, since the technology is still new, there might be security vulnerabilities in particular implementations of it, or undiscovered problems in the infrastructure itself. Salvatore Stolfo, professor of computer science at Columbia University and the founder and CTO at Allure Security Technology, calls it a "target-rich opportunity for sophisticated attackers." "Personally, I wouldn't speculate in those currencies on the exchanges just yet," he says.

Bitcoin still rules for criminal-to-consumer transactions

Bitcoin has a lot of name recognition with the public, and there are more places to buy it. So ransomware authors typically demand that their victims pay them in Bitcoin. "So far as ransomware campaigns using Monero right off the bat, I can't think of any," says Karl Sigler, threat intelligence manager at Trustwave Holdings, Inc. Most of the larger, more legitimate cryptocurrency exchanges don't support Monero at all, he says.

That situation can change rapidly, as well. "I think the only thing the criminals are waiting for are hard-currency to Monero exchanges," says John Bambenek, threat systems manager at Fidelis Cybersecurity, "where you can send victims ransom demands and they can go online with their credit card and purchase the cryptocurrency necessary to pay."

Join the newsletter!

Hunting for Hackers - Why Preventive Measures are Only Part of the Cyber Solution, Duncan Alderson, Senior Manager, Cyber & Forensics, PwC Australia | IDG Security Day

Hunting for Hackers - Why Preventive Measures are Only Part of the Cyber Solution, Duncan Alderson, Senior Manager, Cyber & Forensics, PwC Australia | IDG Security Day

[▶ PLAY VIDEO](#)



Interview with David Sykes, Business Leader, Sophos | IDG Security Day

Interview with David Sykes, Business Leader, Sophos | IDG Security Day

[▶ PLAY VIDEO](#)



Showreel | IDG Security Day conference, 21st June

Showreel | IDG Security Day conference, 21st June

[▶ PLAY VIDEO](#)



Tools of the Trade: A Live Hacking Demonstration - Ty Miller, Director, Threat Intelligence | IDG Security Day

Tools of the Trade: A Live Hacking Demonstration - Ty Miller, Director, Threat Intelligence | IDG Security Day

[▶ PLAY VIDEO](#)



Publisher's Panel - Using AI for next-generation Cyber Security | IDG Security Day

Publisher's Panel - Using AI for next-generation Cyber Security | IDG Security Day

[▶ PLAY VIDEO](#)

[More videos ▶](#)

Blog Posts

Top 3 Targeted CyberAttacks in 2017

Paul Colmer

[Join](#)

Or

[Sign in with LinkedIn](#)[Sign in with Facebook](#)

Check out the really important new feature of the iPhone application in Gmail

Ritesh Mehta

Are all proxies actually security assets?

Matthew Hackling

Awareness

Matt Tett

CSO WANTED

Have an opinion on security? Want to have your articles published on CSO? Please contact CSO Content Manager for our guidelines.

[More about](#)[Akamai Technologies](#)[CrowdStrike](#)[Europol](#)[Inc.](#)[Juniper Networks](#)[Lastline](#)[Masergy Communications](#)[Norton](#)[Synopsys](#)[Technology](#)[Trustwave](#)

Read next



The global cyber war is heating up: Why businesses should be worried



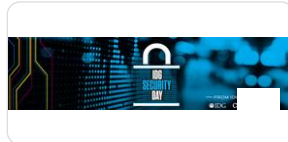
Corporates on notice as nation-state attackers refine tactics, look beyond political disruption



Cybersecurity Threats in the Age of IoT



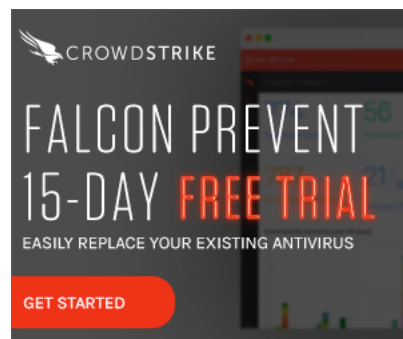
In Pictures: ZertoCON 2017 Sydney



IDG Security Day: Sydney infosec leaders



Cybersecurity Insights - People



0 Comments

CSO Australia

 Login ▾

 Recommend

 Share

Sort by Best ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

Be the first to comment.

 Subscribe

 Add Disqus to your siteAdd DisqusAdd

 Privacy



[Send Us E-mail](#) | [Privacy Policy \[Updated 23 May 17\]](#) | [Subscribe to emails](#) | [Contacts](#)

Copyright 2018 IDG Communications. ABN 14 001 592 650. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of IDG Communications is prohibited.

IDG Sites: [PC World](#) | [GoodGearGuide](#) | [Computerworld Australia](#) | [CIO](#) | [CMO](#) | [Techworld](#) | [ARN](#) | [CIO Executive](#)